UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

GRZEGORZ KAZMIERCZAK, individually and on behalf of all others similarly situated, Plaintiff, v. **COMMUNITY LOAN SERVICING, LLC,** Defendant.	Case No. 1:22-cv-05014 **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiff GZEGORZ KAZMIERCZAK ("Plaintiff"), individually and on behalf of all others similarly situated ("Plaintiff"), through his attorneys, brings this action against Defendant COMMUNITY LOAN SERVICING, LLC ("Defendant"), and alleges upon personal knowledge as to his own actions and experiences, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. This consumer data breach lawsuit arises out of Defendant's unreasonable, unlawful, and unfair practices with regard to its collection and maintenance of highly sensitive and confidential personal and financial information, including names, Social Security numbers, and information provided in connection with loans (the "PII"). Defendant's insufficient and unreasonable data security practices caused, facilitated, and exacerbated the data breach and its impact on Plaintiff and Class members. By Defendant's own admission, from at least October 27,

2021 to December 7, 2021, an unauthorized person obtained access to files on Defendant's file storage servers (the "Data Breach"). Defendant identified the incident in early December 2021. Although Defendant "immediately" notified law enforcement and engaged a forensic investigation firm, Defendant waited nine (9) months to warn those most at risk—Plaintiff and Class members.

2. The Data Breach exposed Plaintiff's and Class members' highly personally identifiable information and financial information ("PII") to criminals, including their names, Social Security numbers, information provided in connection with a loan application, loan modification, and other items regarding loan servicing.

3. The PII that Defendant compromised, exposed, and criminals stole in the Data Breach consists of some of the most sensitive and damaging information when in the hands of criminals, including but not limited to: names, mortgage property address, mortgage account number(s) and mortgage account information, phone number, property information, Social Security numbers, financial account information, account balances and payment history, credit history, credit scores, and home insurance information. Moreover, the information relates to what is for many the single most important asset, both subjectively and objectively—their home.

4. The PII stolen in the Data Breach can be used by criminals alone, and in conjunction with other pieces of information, to perpetrate crimes against Plaintiff and Class members that can result in significant liability and damage to their money, property, creditworthiness, reputation, and their ability to pay current loans, improve their credit, and/or obtain loans on favorable terms in the future.

5. Plaintiff and Class members entrusted Defendant with an extensive amount of their sensitive PII. Defendant understands the importance of protecting such information and touts its

cybersecurity capabilities as a selling point. For example, on its website and in written documents provided to Plaintiff and Class members, Defendant states:

> Community Loan Servicing, LLC recognizes the importance of keeping the personal information you provide to us private and secure. Community Loan Servicing, LLC has developed a comprehensive privacy policy and we use the latest technology to ensure that your personal information is secure.
>
> Privacy Statement
>
> The personal, private information you provide to Community Loan Servicing, LLC will be used in connection with processing, underwriting, funding and servicing the loan for which you applied for. Community Loan Servicing, LLC does not share any information about you or your company to unaffiliated third parties, except as necessary to process, underwrite, fund and service your loan and as permitted by law. Community Loan Servicing, LLC may share information regarding your transaction and account experience, including name and payment history, among our affiliated financial services companies to better serve your needs and notify you of financial services that might interest you, as permitted by applicable law. Community Loan Servicing, LLC does not share, distribute, sell or otherwise disseminate any information about you or your company, except as detailed above.[1]

6. Defendant's Privacy Notice[2] contains the industry standard, regulation-sanctioned information that it provided to Plaintiff and all Class members:

[1] https://communityloanservicing.com/privacy/

[2] https://www.communityloanservicing.com/wp-content/uploads/NL009-CLS-Privacy-Notice-2020.pdf

rev. Sept. 2020

FACTS

WHAT DOES COMMUNITY LOAN SERVICING DO WITH YOUR PERSONAL INFORMATION?
PRIVACY NOTICE / OPT OUT MAIL-IN FORM

Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: o Social Security number and income o Account balances and payment history o Credit history and credit scores
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons Community Loan Servicing, LLC (CLS) chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does CLS share?*	Can you limit this sharing?
For our everyday business purposes--- such as to process your transaction, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus	Yes	No
For our marketing purposes--- to offer our products and services to you	Yes	No
For joint marketing with other financial companies	Yes	No
For our affiliates' everyday business purposes--- information about your transactions and experiences	Yes	No
For our affiliates' everyday business purposes--- information about your creditworthiness	Yes	Yes
For our affiliates to market to you	Yes	Yes
For non-affiliates to market to you	Yes	Yes

*We do not share personal information in connection with the collection of a debt, except as permitted by law.

7. These representations concerning privacy practices and data security were false. On or before October 27, 2021, criminals breached Defendant's inadequately defended systems, and accessed and acquired electronic files containing the PII of Plaintiff and Class members. The criminals gained unauthorized access by thwarting, circumventing, and defeating Defendant's unreasonably deficient data security measures and protocols.

8. Plaintiff, individually, and on behalf of all persons similarly situated, seeks to be made whole for the losses incurred by Plaintiff and the victims of the Data Breach, and the losses that will be incurred in the future. Plaintiff also seek injunctive relief in the form of compliant data security practices, full disclosure regarding the disposition of the information in Defendant's systems, and monitoring and audits of Defendant's security practices going forward because

Defendant continues to collect, maintain, and store Plaintiff's and Class members' PII and home loan data.

PARTIES, JURISDICTION, AND VENUE

9. Plaintiff is a citizen of Illinois.

10. Defendant is a Delaware limited liability company with its principal place of business in Coral Gables, Florida.

11. The Court has original jurisdiction under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d)(2), because this is a Class action involving 100 or more Class members and the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Many members of the Class, including Plaintiff, are citizens of different states from Defendant.

12. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2), as a substantial part of the events giving rise to the claims emanated from activities within this District, and Defendant conducts substantial business in this District.

GENERAL ALLEGATIONS

The Data Breach

13. In its August 30, 2022 notice to Plaintiff and Class members ("Notice Letter"), Defendant states that an unauthorized person obtained access to Defendant's file storage servers containing the PII of Plaintiff and Class members. A true and correct copy of the Notice Letter sent to Plaintiff is attached as Exhibit 1.

14. Information pertaining to Plaintiff's and Class members' mortgage loans was part of the data acquired by an unauthorized persons in the Data Breach.

15. The Notice Letter states that Plaintiff's and Class members' names, Social Security numbers, information provided in connection with a loan application, loan modification, and other

items regarding loan servicing were accessed by unauthorized persons in the Data Breach. The specific information encompassed by these broad categories is unknown to Plaintiff at this time, but likely includes any and all information Defendant collected in carrying out its loan servicing duties, such as financial account information, account balances and payment history, mortgage loan information, property information, taxation information, insurance information, and credit information.

16. Since discovering the Data Breach, Defendant took additional steps to enhance its security measures—actions that should have been employed in the first place—and which would have prevented or limited the impact of the Data Breach.

17. Nine (9) months after Defendant discovered the Data Breach and notified law enforcement, Defendant publicly announced the Data Breach and notified those who were placed at risk of identity theft. Defendant sent notices to persons whose PII was acquired by criminals in the Data Breach.

18. Defendant advised in the Notice Letter that Plaintiff and Class members should obtain credit monitoring and identity theft protection services to help them detect possible misuse of PII. *See* Exhibit 1.

19. As a result of the Data Breach, Plaintiff and Class members have been and must continue to be vigilant and review their credit reports for incidents of identity theft, and educate themselves about security freezes, fraud alerts, and other steps to protect themselves against identity theft. Defendant's Notice Letter also advises Plaintiff and Class members to do all of this.

Industry Standards for Data Security

20. Defendant is aware of the importance of safeguarding Plaintiff's and Class members' PII, that by virtue of its business it places Plaintiff's and Class members' PII at risk of

being targeted by hackers.

21. Defendant is aware that the PII that it collects, organizes, and stores, can be used by criminals to engage in crimes such as identity fraud and theft using Plaintiff's and Class members' PII.

22. Because of Defendant's failure to implement, maintain, and comply with necessary cybersecurity requirements, Defendant was unable to protect Plaintiff's and Class members' information and confidentiality, and protect against obvious and readily foreseeable threats to information security and confidentiality. As a proximate result of such failures, criminals gained unauthorized access to Defendant's network unimpeded for six (6) weeks, and acquired Plaintiff's and Class members' personal and financial information in the Data Breach without being stopped.

23. Only after the attack was completed did Defendant begin to undertake basic steps recognized in the industry to protect Plaintiff's and Class members' PII.

24. Defendant was unable to prevent the Data Breach, and was unable to detect the unauthorized access to vast quantities of sensitive and protected files containing protected information of Plaintiff and Class members for six (6) weeks. Discovery on Defendant, law enforcement investigators, and private investigators, will reveal more specific facts about Defendant's deficient and unreasonable security procedures.

25. Security standards commonly accepted among businesses that store personal and financial information using the Internet include, without limitation:

a) Maintaining a secure firewall configuration;

b) Monitoring for suspicious or irregular traffic to servers;

c) Monitoring for suspicious credentials used to access servers;

d) Monitoring for suspicious or irregular activity by known users;

e) Monitoring for suspicious or unknown users;

f) Monitoring for suspicious or irregular server requests;

g) Monitoring for server requests for personal and financial information;

h) Monitoring for server requests from VPNs; and

i) Monitoring for server requests from Tor exit nodes.

26. The U.S. Federal Trade Commission ("FTC") publishes guides for businesses for cybersecurity[3] and protection of personal and financial information[4] which includes basic security standards applicable to all types of businesses.

27. The FTC recommends that businesses:

a) Identify all connections to the computers where you store sensitive information;

b) Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks;

c) Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business;

d) Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine;

e) Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks;

---

[3] *See* F.T.C., *Start with Security: A Guide for Business*, (June 2015), https://www.ftc.gov/system/files/ documents/plain-language/pdf0205-startwithsecurity.pdf (*last accessed* July 23, 2020).

[4] *See* F.T.C., *Protecting Personal Information: A Guide for Business*, (Oct. 2016), https://www.ftc.gov/ system/files/documents/plain-language/pdf-0136_protecting personalinformation.pdf (*last accessed* July 23, 2020).

f) Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet;

g) Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically;

h) Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day; and

i) Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

28. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[5]

29. Because Defendant was entrusted with consumers' personal and financial information, it had and has a duty to keep the PII secure.

[5] F.T.C., *Privacy and Security Enforcement: Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (*last accessed* July 15, 2020).

30. Plaintiff and Class members reasonably expect that when they provide their personal and financial information to a company, the company will safeguard their personal and financial information.

31. Despite Defendant's obligations, Defendant failed to upgrade and maintain its data security systems in a meaningful way so as to prevent the Data Breach.

32. Specifically, in breach of its duties, Defendant failed to:

a) Replace email filtering tools, malware software, and Internet monitoring tools with more robust solutions that utilize artificial intelligence ("AI") to detect and block known and newly introduced malware;

b) Block all inbound and outbound Internet, email, and network traffic to foreign countries;

c) Maintain a secure firewall configuration;

d) Monitor for suspicious or irregular traffic to servers;

e) Monitor for suspicious credentials used to access servers;

f) Monitor for suspicious or irregular activity by known users;

g) Monitor for suspicious or unknown users;

h) Monitor for suspicious or irregular server requests;

i) Monitor for server requests for personal and financial information;

j) Monitor for server requests from VPNs;

k) Monitor for server requests from Tor exit nodes;

l) Identify all connections to the computers where Defendant stores sensitive information;

m) Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks;

n) Scan computers on Defendant's network to identify and profile the operating system and open network services, and disable services that are not needed to prevent hacks or other potential security problems;

o) Pay particular attention to the security of Defendant's web applications—the software used to give information to visitors to its websites and to retrieve information from them;

p) Use a firewall to protect Defendant's computers from hacker attacks while they are connected to a network, especially the Internet;

q) Not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting its business;

r) Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically;

s) Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day; and

t) Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

33. Defendant negligently entrusted duties to safeguard Plaintiff's and Class members' PII to contractors without adequately monitoring, inspecting, and controlling their data security practices.

34. Defendant negligently supervised contractors and failed to require them to implement, maintain, and upgrade sufficiently its data security systems and protocols.

35. Had Defendant properly maintained its systems and adequately protected them, they could have prevented the Data Breach.

Defendant Owed Duties to Plaintiff and Class Members to Adequately Safeguard Their PII

36. Defendant is aware of the importance of security in maintaining personal information (particularly sensitive personal and financial information), and the value consumers place on keeping their PII secure.

37. Defendant owes duties to Plaintiff and the Class members to maintain adequate security and to protect the confidentiality of their PII.

38. Defendant owes a further duty to its customers to immediately and accurately notify them of a breach of its systems to protect them from identity theft and other misuse of their personal data and to take adequate measures to prevent further breaches.

The Categories of PII at Issue Here Are Particularly Valuable to Criminals

39. Businesses that solicit, aggregate, and store sensitive PII are likely to be targeted by cyber criminals. Credit card and bank account numbers are tempting targets for hackers. However, information such as Social Security numbers are even more attractive to hackers because they are not easily destroyed and can be easily used to perpetrate identity theft and other types of fraud.

40. The unauthorized disclosure of Social Security numbers can be particularly damaging, because Social Security numbers cannot easily be replaced. In order to obtain a new Social Security number a person must prove, among other things, that he or she continues to be disadvantaged by the misuse. Thus, no new Social Security number can be obtained until the damage has been done.

41. Furthermore, as the Social Security Administration ("SSA") warns:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number.

> Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[6]

42. Here, the unauthorized access by the hackers left the cyber criminals with the tools to perform the most thorough identity theft—they have obtained all the essential PII to mimic the identity of the user. Plaintiff's and Class members' stolen personal data represents essentially one-stop shopping for identity thieves.

43. According to the FTC, identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.[7] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.[8]

44. More recently the FTC has released its updated publication on protecting PII for businesses, which includes instructions on protecting PII, properly disposing of PII, understanding network vulnerabilities, implementing policies to correct security problems, using intrusion

---

[6] SSA, Identity Theft and Your Social Security Number, SSA Publication No. 05-10064 (Dec. 2013), *available at* http://www.ssa.gov/pubs/EN-05-10064.pdf (last visited 3/26/2021).

[7] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (2012), http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf (last visited 3/26/2021).

[8] *Id.* The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

detection programs, monitoring data traffic, and having in place a response plan.

45. The FTC has, upon information and belief, brought enforcement actions against businesses for failing to protect PII. The FTC has done this by treating a failure to employ reasonable measures to protect against unauthorized access to PII as a violation of the FTC Act, 15 U.S.C. § 45.

46. General policy reasons support such an approach. A person whose personal information has been compromised may not see any signs of identity theft for *years*. According to a U.S. Government Accountability Office report:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[9]

47. Companies recognize that PII is a valuable asset. Indeed, PII is a valuable commodity. A "cyber black-market" exists in which criminals openly post stolen Social Security numbers and other PII on a number of Internet websites. Plaintiff's and Class members' personal data that was stolen has a high value on both legitimate and black markets.

48. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information as follows:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[10]

---

[9] *See* http://www.gao.gov/new.items/d07737.pdf at 29 (last visited 11/13/2020).

[10] FEDERAL TRADE COMMISSION, *The Information Marketplace: Merging and Exchanging Consumer Data*, *transcript available* at http://www.ftc.gov/news-events/events-calendar/2001/03/information-marketplace-merging-exchanging-consumer-data (last visited 11/13/2020).

49. Individuals rightfully place a high value not only on their PII, but also on the privacy of that data. Researchers have already begun to shed light on how much individuals value their data privacy—and the amount is considerable.

50. Notably, one study on website privacy determined that U.S. consumers valued the restriction of improper access to their personal information—the very injury at issue here—between $11.33 and $16.58 per website. The study also determined that "[a]mong U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth US$30.49 – 44.62."[11] This study was done in 2002. The sea-change in how pervasive the Internet is in everyday lives since then indicates that these values—when associated with the loss of PII to bad actors—would be exponentially higher today.

51. Identity thieves may commit various types of crimes such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, and/or using the victim's information to obtain a fraudulent tax refund or fraudulent unemployment benefits. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

52. To date, Defendant has offered Plaintiff and Class members only one year of identity theft detection services. The offered service is wholly inadequate to protect Plaintiff and Class members from the threats they face for years to come, particularly in light of the PII at issue here, and is not an adequate cure of the Data Breach.

53. As noted above, the disclosure of Social Security numbers in particular poses a significant risk. Criminals can, for example, use Social Security numbers to create false bank

[11] Hann, Hui, *et al*, The Value of Online Information Privacy: Evidence from the USA and Singapore, at 17. Oct. 2002, available at https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last visited 3/26/2021).

accounts or file fraudulent tax returns.[12] Plaintiff and Class members will and already have spent time contacting various agencies, such as the Internal Revenue Service and the Social Security Administration. They also now face a real and imminent substantial risk of identity theft and other problems associated with the disclosure of their Social Security number and will need to monitor their credit and tax filings for an indefinite duration.

54. Again, because the information Defendant allowed to be compromised and taken is of such a durable and near-permanent quality, the harms to Plaintiff and the Class will continue to grow, and Plaintiff and Class members will continue to be at substantial risk for further imminent and future harm.

Damages From Data Breaches

55. According to Javelin Strategy & Research, in 2017 alone over 16.7 million individuals were affected by identity theft, causing $16.8 billion to be stolen.

56. Consumers place a high value not only on their personal and financial information, but also on the privacy of that data. This is because identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.

57. The United States Government Accountability Office explains that "[t]he term 'identity theft' is broad and encompasses many types of criminal activities, including fraud on existing accounts—such as unauthorized use of a stolen credit card number—or fraudulent creation of new accounts—such as using stolen data to open a credit card account in someone else's name." *See In re Zappos.com, Inc.*, 888 F.3d 1020, 1024 (9th Cir. 2018). The GAO Report

[12] When fraudulent tax returns are filed, the requirements for a legitimate taxpayer to file their tax returns with the IRS increase, including the necessity to obtain and utilize unique PIN numbers just to be able to file a tax return.

notes that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."

58. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports often, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.

59. Identity thieves use stolen personal and financial information for "various types of criminal activities, such as when personal and financial is used to commit fraud or other crimes," including "credit card fraud, phone or utilities fraud, bank fraud and government fraud." *In re Zappos.com, Inc.*, 888 F.3d at 1024. The information exfiltrated in the Data Breach can also be used to commit identity theft by placing Plaintiff and Class members at a higher risk of "phishing," "vishing," "smishing," and "pharming," which are which are ways for hackers to exploit information they already have to get even more personally identifying information through unsolicited email, text messages, and telephone calls purportedly from a legitimate company requesting personal, financial, and/or login credentials.

60. There may be a time lag between when harm occurs versus when it is discovered, and also between when personal and financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

61. Personal and financial information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber blackmarket" for years.

62. Thus, there is a strong probability that entire batches of stolen information have been dumped on the black market, or are yet to be dumped on the black market, meaning Plaintiff and Class members are at an increased risk of fraud and identity theft for many years into the future.

63. Data breaches are preventable. As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions." She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."

64. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a data breach never occurs."

65. Indeed, here Defendant deployed enhanced security monitoring tools across its network after the Data Breach, but should have implemented them to prevent the Data Breach.

66. The types of information Defendant acknowledges were stolen by the criminals are sufficiently sensitive and valuable to identity thieves and criminals in perpetrating identity crimes. Defendant states that Plaintiff's and Class members' names, Social Security numbers, and

information connected to loan applications, modifications, and other loan servicing information were accessed and acquired, which would include: mortgage property address, mortgage account number(s) and mortgage account information, phone number, property information, insurance information, taxation information, credit history, credit scores, account balances and payment history, home insurance policy number, and home insurance information were accessed and acquired. *See* Exhibit 1. Much if not all of this information is essentially immutable and can be used to perpetrate scams, victimize the persons who own the information, and commit identity theft and fraud.

67. The types of information compromised in the Data Breach are immutable. Plaintiff and Class members are not able to change them or simply cancel them, like a credit card, to avoid harm or fraudulent use of the information. Just like a birthdate or a mother's maiden name, these pieces of information cannot be changed by logging into a website and changing them in settings, and they can be used alone or in conjunction with other pieces of information to commit serious fraud.

68. Criminals can use the information to devise and employ phishing and social engineering schemes capitalizing on the genuine information stolen from Defendant to send fraudulent mail, emails, and other communications to Plaintiff and Class members that look authentic, but which are designed to lure them into paying money or providing other information that the criminals can use to steal money. For example, homeowners with trouble paying their loan payments may experience scams targeting them.

69. According to Experian:[13]

Mortgage Foreclosure Relief and Debt Management Scams

[13] https://www.experian.com/blogs/ask-experian/heres-everything-you-need-to-know-about-the-risks-of-mortgage-fraud/ (last visited March 30, 2022).

> In this type of mortgage fraud, scammers contact homeowners offering help if they can't make payments or may be falling behind on their mortgage (the primary contact is by phone with these). … Often they make promises of lower payments or making the payments for a homeowner in exchange for rent payments to their company. However, they don't actually make the mortgage payments and you may end up going into foreclosure anyway.
>
> Also known as foreclosure scams or foreclosure rescue schemes, this kind of fraud is unfortunately very common and can cost consumers a lot of Money.

70. The information stolen in the Data Breach, by itself, can also be used by criminals to perpetrate fraud that will leave Plaintiff and Class members holding the bag. Experian explains that certain scams, including mortgage fraud, can be effectively perpetrated using only a name and loan number.[14]

> How Consumers Are Affected By Mortgage Fraud
>
> Identity theft is a particularly threatening form of mortgage fraud, as it tends to lead directly toward homeowner financial loss. For example, if an identity thief steals a homeowner's Social Security number, or intercepts the mortgage account number, he or she can use that information to take out a home equity line of credit (also known as a HELOC) worth tens of thousands of dollars, in the homeowner's name.

71. Experian explains how mortgage fraud impacts the homeowner. When the credit is provided to the fraudster:[15]

> The cash is sent to a fraudulent account established by the thief, and the homeowner is left holding the bill. Or, the fraudster could take out a second mortgage using the homeowner's stolen data information, and escape with the cash, once again leaving the debt to the homeowner.
>
> While any form of mortgage fraud is a serious offense, losing one's data to identity thieves can trigger a financial loss that's difficult to overcome, and that could take years to clear. Additional impacts include losing money, time, or missing out on the purchase of a dream home because you have to take additional time to deal with restoring your identity if you're the victim of mortgage fraud.

[14] *Id.*
[15] *Id.*

72. Identity Force explains what a thief or scammer can do with sensitive information, such as loan information and identifying details, including stealing your home:[16]

> Mortgaging Your Good Name
>
> Mortgage fraud through identity theft is a very real risk. A thief can steal your Social Security number and other identifying details, then pretend to be you to a bank or mortgage broker. The criminal might refinance your home for more than what's owed and then take the extra cash or obtain a home equity line of credit and drain that account.
>
> In some cases, you can experience house stealing through a fraudulent deed transfer. An identity thief could use stolen information to execute a transfer, which would put your property in his or her name. That means you'd legally no longer own that real estate. Since the criminal's name is on the deed, he or she would have the right to take out loans against the house. With no payments made on those loans or the mortgage, the property could even go into foreclosure.
>
> Thieves can get the information they need for these transactions by stealing your mail, getting personal details through fraudulent phone calls, or making copies of your driver's license to impersonate you. Unfortunately, sometimes it's friends and family who are the culprits (known as familiar fraud) since they may have access to files inside a home and often know many of the personal details required to impersonate you.

Plaintiff Received Defendant's Data Breach Notification Letter

73. Plaintiff took out a mortgage loan for property in Illinois. For all times relevant to this Complaint, Defendant was the servicer of the loan.

74. Plaintiff and Class members provided Defendant with significant personal, income, and financial information that Defendant was able to acquire and to supplement by obtaining credit reports and banking information from third parties. Such information included, but is not limited to:

- Full name, mailing address, phone numbers, email address, and loan identification number;
- Co-borrower contact information, phone numbers, email address, and

[16] https://www.identityforce.com/blog/home-loan-identity-theft. (last visited March 30, 2022)

mailing address;

- Notations and comments concerning collections and loan servicing;
- Fee balance information;
- Information regarding insurance on the property and property details pertinent thereto;
- Loan history information, Social Security number, transaction dates, due dates, transaction amount, principal amount, end principal balance, interest, escrow amounts, check numbers, late charges, assistance amounts, details on loans in arrears;
- Tax information, including tax type, frequency, account number, and payee information;
- Credit information from consumer reports and files held by consumer reporting agencies, including account balances and payment history; and
- Other information, but Plaintiff does not know the full extent of the information Defendant has relating to Plaintiff.

75. It is plausible to assume that the foregoing pieces of information relating to Plaintiff and Class members were exposed, compromised, accessed, viewed without authorization, and stolen in the Data Breach by criminals. Defendant's Notice Letter indicates that broad categories of personal and financial information "regarding loan servicing" were acquired in the Data Breach, but does not provide any more particularity regarding what information those categories encompass.

76. On or about August 30, 2022, Defendant sent the Notice Letter by mail notifying Plaintiff and Class members that PII relating to Plaintiff and other residential mortgage clients—including their names, Social Security numbers, and other mortgage loan related information—was taken by an "unauthorized person" in the Data Breach. *See* Exhibit 1.

Plaintiff's and Class Members' Damages

77. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from

fraud and identity theft.

78. Plaintiff and Class members have or will suffer actual injury as a direct result of the Data Breach including:

a) Spending time reviewing finding fraudulent charges and remedying fraudulent charges;

b) Purchasing credit monitoring and identity theft prevention;

c) Time and money addressing and remedying identity theft;

d) Spending time placing "freezes" and "alerts" with credit reporting agencies and, subsequently, temporarily lifting a security freeze on a credit report, or removing a security freeze from a credit report;

e) Spending time on the phone with or visiting financial institutions to dispute fraudulent charges;

f) Contacting their financial institutions and closing or modifying financial accounts compromised as a result of the Data Breach; and

g) Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

79. Moreover, Plaintiff and the Class members have an interest in ensuring that their personal and financial information is protected from further breaches by the implementation of security measures and safeguards, including making sure that the storage of data containing their personal and financial information is secure.

80. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class members have suffered anxiety, emotional distress, and loss of privacy.

81. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class members are at an increased and immediate risk of future harm, including from identity theft and fraud related to their financial accounts.

82. As a result of the Data Breach, Plaintiff and Class members are at an imminent risk of identity theft and fraud. This risk will continue to exist for years to come, as Plaintiff and Class

members must spend their time being extra vigilant, due to Defendant's failures, to try to prevent being victimized for the rest of their lives.

83. Because Defendant presented such an easy target to cyber criminals, Plaintiff and Class members have already been subjected to violations of their privacy, and have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class members must now and in the future, spend time to more closely monitor their financial accounts to guard against identity theft and other fraud.

84. Plaintiff and Class members may also incur out-of-pocket costs for, among other things, purchasing credit monitoring services or other protective measures to deter and detect identity theft.

CLASS ACTION ALLEGATIONS

85. Plaintiff brings this action pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3) on behalf of a class of similarly situated individuals (the "Class") defined as follows:

> All individuals in the United States whose personally identifiable information was accessed in the Data Breach.

86. In addition, Plaintiff brings this action pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3) on behalf of a subclass of similarly situated individuals in Illinois ("Illinois Subclass") defined as follows:

> All individuals in Illinois whose personally identifiable information was accessed in the Data Breach.

87. Excluded from the Class and Subclass (collectively, "Classes") are Defendant; any entity in which Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by Defendant; and the affiliates, legal representatives, attorneys, heirs, predecessors, successors, and assigns of Defendant. Also excluded are the judges and court personnel in this case and any members of their immediate families.

88. Plaintiff reserves the right to modify and/or amend the Class definitions, including but not limited to creating subclasses, as necessary.

89. ***Numerosity***. The Classes are so numerous that joinder of all members is impracticable. The identities of all Class members are ascertainable through Defendant's records.

90. ***Commonality***. There are numerous questions of law and fact common to Plaintiff and the Classes, including the following:

- Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class members;
- Whether Defendant had a duty not to disclose the PII of Plaintiff and Class members to unauthorized third parties;
- Whether Defendant had a duty not to use the PII of Plaintiff and Class members for non-business purposes;
- Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class members;
- Whether and when Defendant actually learned of the Data Breach;
- Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class members that their PII had been compromised;
- Whether Defendant violated the law by failing to promptly notify Plaintiff and Class members that their PII had been compromised;
- Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class members;
- Whether Plaintiff and Class members are entitled to actual damages, nominal damages, and/or exemplary damages as a result of Defendant's wrongful conduct;
- Whether Plaintiff and Class members are entitled to restitution as a result of Defendant's wrongful conduct; and

- Whether Plaintiff and Class members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

91. ***Typicality***. Plaintiff's claims are typical of the claims of the Classes because Plaintiff, like all Class members, had his personal and financial data compromised, breached and stolen in the Data Breach. Plaintiff and Class members were injured through Defendant's uniform misconduct described in this Complaint and assert the same claims for relief.

92. ***Adequacy***. Plaintiff and his counsel will fairly and adequately protect the interests of the Class. Plaintiff has retained counsel who are experienced in class actions and complex litigation, including data privacy litigation of this kind. Plaintiff has no interests that are antagonistic to, or in conflict with, the interests of other members of the Class.

93. ***Predominance***. The questions of law and fact common to Class members predominate over any questions which may affect only individual members.

94. ***Superiority***. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Moreover, absent a class action, most Class members would find the cost of litigating their claims prohibitively high and would therefore have no effective remedy, so that in the absence of class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go unremedied without certification of the Class. Plaintiff and Class members have been harmed by Defendant's wrongful conduct and/or action. Litigating this action as a class action will reduce the possibility of repetitious litigation relating to Defendant's conduct and/or inaction. No difficulties would be encountered in this litigation that would preclude its maintenance as a class action.

95. Class certification, therefore, is appropriate under Fed. R. Civ. P. 23(b)(3), because the above common questions of law or fact predominate over any questions affecting individual

members of the Class, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

96. Class certification is appropriate under Fed. R. Civ. P. 23(b)(2), because Defendant has acted or refused to act on grounds that apply generally to the Classes so that final injunctive relief or corresponding declaratory relief is appropriate respecting the Class as a whole.

COUNT I
Negligence
(On behalf of Plaintiff and the Class and Illinois Subclass)

97. Plaintiff repeats and realleges the allegations of paragraphs 1-96 with the same force and effect as though fully set forth herein.

98. Defendant's actions and inactions were of the type that would result in foreseeable, unreasonable risk of harm to Plaintiff and Class members. Defendant knew, or should have known, of the risks inherent in collecting and storing the personal and financial information of Plaintiff and Class members and the importance of adequate security in storing the information. Additionally, Defendant is aware of numerous, well-publicized data breaches that exposed the personal and financial information of individuals.

99. Defendant had a common law duty to prevent foreseeable harm to Plaintiff's and Class members' PII. This duty existed because Plaintiff and Class members were the foreseeable and probable victims of the failure of Defendant to adopt, implement, and maintain reasonable security measures so that Plaintiff's and Class members' personal and financial information would not be unsecured and accessible by unauthorized persons.

100. Defendant had a special relationship with Plaintiff and Class members. Defendant was entrusted with Plaintiff's and Class members' personal and financial information, and

Defendant was in a position to protect the personal and financial information from unauthorized access.

101. The duties of Defendant also arose under section 5 of the FTC Act, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect individuals' personal and financial information by companies. Various FTC publications and data security breach orders further form the basis of the duties of Defendant.

102. Defendant had a duty to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Plaintiff's and Class members' personal and financial information in its possession so that the personal and financial information would not come within the possession, access, or control of unauthorized persons.

103. More specifically, the duties of Defendant included, among other things, the following duties, and Defendant carelessly and negligently acted or failed to act in one or more of the following ways:

- Failing to conduct proper and reasonable due diligence over its vendors and contractors and their data security systems, practices, and procedures;
- Failing to conduct proper and reasonable due diligence over vendors or contractors that were the vectors of or facilitated the infiltration into the systems sorting the PII;
- Failing to maintain reasonable and appropriate oversight and audits on vendors or contractors that were the vectors of the Data Breach;
- Failing to adopt, implement, and maintain adequate security measures for protecting an individual's personal and financial information to ensure that the information is not accessible online by unauthorized persons;
- Failing to adopt, implement, and maintain adequate security measures for deleting or destroying personal and financial information when Defendant's business needs no longer required such information to be stored and maintained; and

- Failing to adopt, implement, and maintain processes to quickly detect a data breach and to promptly act on warnings about data breaches, and notify affected persons without unreasonable delay.

104. Defendant breached the foregoing duties to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting personal and financial information in its possession so that the information would not come within the possession, access, or control of unauthorized persons.

105. Defendant acted with reckless disregard for the security of the personal and financial information of Plaintiff and Class members because Defendant knew or should have known that its data security was not adequate to safeguard the personal and financial information that was collected and stored.

106. Defendant acted with reckless disregard for the rights of Plaintiff and the Class members by failing to promptly detect the Data Breach, and further, by failing to notify Plaintiff and the Class members of the Data Breach in the most expedient time possible and without unreasonable delay pursuant to common law duties to provide reasonably timely and truthful data-breach notification, so that Plaintiff and Class members could promptly take measures to protect themselves from the consequences of the unauthorized access to the personal and financial information compromised in the Data Breach.

107. As a result of the conduct of Defendant, Plaintiff and Class members have suffered and will continue to suffer foreseeable harm. Plaintiff and Class members have suffered actual damages including, but not limited to, imminent risk of identity theft; expenses and/or time spent on credit monitoring for a period of years; time spent scrutinizing bank statements, credit card statements, and credit reports; time spent initiating fraud alerts and credit freezes and subsequently temporarily lifting credit freezes; and increased risk of future harm. Further, Plaintiff and Class

members have suffered and will continue to suffer other forms of injury and/or harm including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT II
Negligence Per Se
(On Behalf of Plaintiff and the Class and Illinois Subclass)

108. Plaintiff repeats and reallegess the allegations of paragraphs 1-96 with the same force and effect as though fully set forth herein.

109. "Section 5 of the FTC Act [15 U.S.C. § 45] is a statute that creates enforceable duties, and this duty is ascertainable as it relates to data breach cases based on the text of the statute and a body of precedent interpreting the statute and applying it to the data beach context." *In re Capital One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 407 (E.D. Va. 2020). "For example, in *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 240 (3d Cir. 2015), the United States Court of Appeals for the Third Circuit affirmed the FTC's enforcement of Section 5 of the FTC Act in data breach cases." *Capital One Data Security Breach Litigation*, 488 F. Supp. 3d at 407.

110. In addition, Plaintiff and Class members may maintain a negligence per se claim based on conduct declared unlawful under the Safeguards Rule, 16 C.F.R. part 314, promulgated by the FTC pursuant to authority delegated by Congress under the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6801(b), to establish standards for financial institutions relating to administrative, technical, and physical safeguards for nonpublic information, including Plaintiff's and Class members' PII.

111. The Safeguards Rule at 16 C.F.R. § 314.4 provides:

> In order to develop, implement, and maintain your information security program, [a financial institution] shall:
>
> (a) Designate an employee or employees to coordinate your information security program.
>
> (b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:
>
> (1) Employee training and management;
>
> (2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and
>
> (3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.
>
> (c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

> (d) Oversee service providers, by:
>
> (1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and
>
> (2) Requiring your service providers by contract to implement and maintain such safeguards.
>
> (e) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.
>
> 16 C.F.R. § 314.4.

112. The Safeguards Rule is a process-based rule drafted using intentionally broad language and not incorporating any specific information security standard or framework to allow financial institutions flexibility to "shape the information security programs to their particular business and to allow the programs to adapt to changes in technology and threats to the security and integrity of customer information."[17]

113. Defendant is a financial institution within the meaning of the GLBA.

114. Plaintiff's and Class members' PII was and is nonpublic personal information and customer information.

[17] Fed. Trade Comm'n, Standards for Safeguarding Customer Information, 84 Fed. Reg. 13158, 13159 (Apr. 4, 2019), also available at https://www.federalregister.gov/documents/2019/04/04/2019-04981/standards-for-safeguarding-customer- information (last visited Nov. 16, 2021).

115. Defendant committed unlawful acts by failing to comply with the requirements of the Safeguards Rule, including but not limited to, failing to:

- Upgrade and maintain data security systems in a meaningful way so as to prevent the Data Breach;
- Replace email filtering tools, malware software, and Internet monitoring tools with more robust solutions that utilize artificial intelligence ("AI") to detect and block known and newly introduced malware;
- Block all inbound and outbound Internet, email, and network traffic to foreign countries;
- Maintain a secure firewall configuration;
- Monitor for suspicious or irregular traffic to servers;
- Monitor for suspicious credentials used to access servers;
- Monitor for suspicious or irregular activity by known users;
- Monitor for suspicious or unknown users;
- Monitor for suspicious or irregular server requests;
- Monitor for server requests for personal and financial information;
- Monitor for server requests from VPNs;
- Monitor for server requests from Tor exit nodes;
- Identify all connections to the computers where Defendant stores sensitive information;
- Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks;
- Scan computers on Defendant's network to identify and profile the operating system and open network services, and disable services that are not needed to prevent hacks or other potential security problems;
- Pay particular attention to the security of Defendant's web applications—the software used to give information to visitors to its websites and to retrieve information from them;
- Use a firewall to protect Defendant's computers from hacker attacks while they are connected to a network, especially the Internet;

- Not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting its business;

- Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically;

- Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day; and

- Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

116. Plaintiff and Class members are in the group of persons the FTC Act and Safeguards Rule were enacted and implemented to protect, and the harms they suffered in the Data Breach as a result of Defendant's violations of the FTC Act and Safeguards Rule were the types of harm they were designed to prevent.

117. As a result of the conduct of Defendant that violated the FTC Act and the Safeguards Rule, Plaintiff and Class members have suffered and will continue to suffer foreseeable harm. Plaintiff and Class members have suffered actual damages including, but not limited to, imminent risk of identity theft; expenses and/or time spent on credit monitoring for a period of years; time spent scrutinizing bank statements, credit card statements, and credit reports; time spent initiating fraud alerts and credit freezes and subsequently temporarily lifting credit freezes; and increased risk of future harm. Further, Plaintiff and Class members have suffered and will continue

to suffer other forms of injury and/or harm including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiff and the Class and Illinois Subclass)

118. Plaintiff repeats and realleges the allegations of paragraphs 1-96 with the same force and effect as though fully set forth herein.

119. Defendant acquired and maintained the PII of Plaintiff and Class members.

120. At the time Defendant acquired the PII of Plaintiff and Class members, there was a meeting of the minds and a mutual understanding that Defendant would safeguard the PII using reasonable security measures and not take unjustified risks when collecting, digitizing, and storing the PII.

121. Plaintiff and Class members would not have entrusted their PII to Defendant had they known that Defendant would make the PII vulnerable and fail to take reasonable precautions, such as encrypting the data while in storage, and deleting PII that was no longer necessary.

122. Defendant promised to comply with industry standards and to ensure that Plaintiff's and Class members' PII would remain protected.

123. Implicit in the agreements between Plaintiff and Class members and Defendant to provide PII was Defendant's obligation to:

- Use the PII for business purposes only;
- Take reasonable steps to protect and safeguard the PII from known and foreseeable risks;
- Prevent unauthorized disclosures of the PII;

- Provide Plaintiff and Class members with prompt and sufficient notice of instances where unauthorized access to the PII is reasonably suspected;
- Reasonably safeguard and protect the PII of Plaintiff and Class members from unauthorized disclosures or uses;
- Ensure vendors and contractors employ robust and industry standard data security procedures and practices;
- Monitor and audit vendors and contractors to ensure compliance with reasonable and industry standard data security procedures and practices.

124. In collecting and maintaining the PII of Plaintiff and Class members and publishing and disseminating privacy notices, Defendant entered into contracts to protect and keep security over the PII of Plaintiff and Class members.

125. Plaintiff and Class members fully performed under their contract with Defendant.

126. Defendant breached the contracts by failing to protect and keep private financial information of Plaintiff and Class members, including by failing to: (i) encrypt or tokenize the sensitive PII of Plaintiff and Class members, (ii) delete such PII that Defendant no longer had reason to maintain, (iii) eliminate the potential accessibility of the PII from the Internet where such accessibility was not justified, and (iv) otherwise review and improve the security of the network system that contained such PII.

127. Defendant also breached a duty to provide reasonably expedient and sufficient notification of the Data Breach.

128. As a result of Defendant's breach of implied contract, Plaintiff and Class members have suffered and will continue to suffer foreseeable harm. Plaintiff and Class members have suffered actual damages including, but not limited to, imminent risk of identity theft; expenses

and/or time spent on credit monitoring for a period of years; time spent scrutinizing bank statements, credit card statements, and credit reports; time spent initiating fraud alerts and credit freezes and subsequently temporarily lifting credit freezes; and increased risk of future harm. Further, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT IV
Violation of Illinois Consumer Fraud and Deceptive Business Practices Act ("ICFA"), 815 ILCS 505/1, *et seq*.
(On Behalf of Plaintiff and the Class and the Illinois Subclass)

129. Plaintiff re-alleges and incorporates by reference paragraphs 1–96 as if fully set forth herein.

130. As a corporation that collects, handles, stores, and maintains patient information that is nonpublic and personally identifiable information, Defendant is a data collector within the meaning of 815 ILCS 530/5.

131. As a data collector, Defendant is required to implement and maintain reasonable security measures to protect Plaintiff's and Class members' PII from unauthorized access, acquisition, destruction, use, modification, or disclosure. 815 ILCS 530/45.

132. Defendant breached these duties and the applicable standards of care by:

- Failing to conduct proper and reasonable due diligence and oversight over employees, agents, and vendors who have access to PII and its data security systems, practices, and procedures;
- Failing to conduct proper and reasonable due diligence over the employees, agents, and vendors who were the vector(s) of and/or facilitated the hackers' infiltration into the system(s) storing Plaintiff's and Class members' PII;

- Failing to maintain reasonable and appropriate oversight and audits on employees, agents, or vendors who were the vectors of the hackers' infiltration into the system(s) storing Plaintiff's and Class members' PII;
- Failing to implement and maintain reasonable safeguards and procedures, such as encryption, to prevent the unauthorized disclosure of Plaintiff's and Class members' PII;
- Failing to monitor and detect its confidential and sensitive data environment(s) storing Plaintiff's and Class members' PII reasonably and appropriately in order to repel or limit the Data Breach;
- Failing to implement and maintain reasonable data storage and retention procedures with respect to the PII to ensure the PII was being stored and maintained for legitimate and useful purposes;
- Failing to undertake reasonable and sufficient incident response measures to ensure that the cyberattack directed toward Defendant's sensitive information would be thwarted and not expose and cause disclosure and unauthorized acquisition of Plaintiff's and Class members' PII;
- Failing to cure deficiencies in data security that allowed the Data Breach to continue, grow in severity and scope, and go undetected and undeterred for additional time;
- Failing to ensure that Plaintiff's and Class members' PII was timely deleted, destroyed, rendered unable to be used, or returned to Plaintiff and Class members;

- Failing to reasonably conduct a forensic investigation into the scope, nature, and exposure of the Data Breach or to ascertain its full severity;
- Failing to provide full disclosure about, and deceptively misleading consumers through false representations and misleading omissions of fact regarding, the Data Breach, consumers' risk and exposure caused by the Data Breach, and the adequacy of the investigation of and response to the Data Breach;
- Failing to provide accurate, complete, and sufficiently detailed notification to Plaintiff and Class members regarding the circumstances of the Data Breach, its causes, its effects, the extent of the exposure of their PII, and details regarding the disposition of Plaintiff's and the other Class members' PII at all times during the Data Breach.

133. Defendant failed to timely notify Plaintiff and Class members that their PII was acquired in the Data Breach. Likely, notification could have been provided in mere days to all the individuals whose names and information was contained in the files that were accessed by the criminals. Instead, Defendant delayed notification for nine (9) months while cyber criminals were able to perpetrate fraud with Plaintiff's and Class members' PII unbeknownst to them long after Defendant became aware of the Data Breach.

134. As a proximate result of Defendant's unfair acts and practices described above and the resulting injuries to Plaintiff and Class members, as herein alleged, Plaintiff and Class members have incurred damages.

135. As a direct and proximate result of Defendant's unlawful acts and omissions, Plaintiff and Class members have suffered actual and concrete injuries and will suffer addition

injuries into the future, including economic and non-economic damages in the following forms: (a) invasion of privacy; (b) financial costs incurred mitigating the imminent risk of identity theft; (c) loss of time and loss of productivity incurred mitigating the imminent risk of identity theft; (d) loss of time and loss of productivity heeding Defendant's warnings and following its instructions in the Notice Letter; (e) financial costs incurred due to actual identity theft; (f) the cost of future identity theft monitoring; (g) loss of time incurred due to actual identity theft; (h) loss of time and annoyance due to increased targeting with phishing attempts and fraudulent robo-calls; and (i) and diminution of value of their PII.

136. Additionally, as a direct and proximate result of Defendant's unlawful conduct, Plaintiff and Class members have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession. Plaintiff and Class members are, therefore, also seeking injunctive relief for the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to safeguard the PII.

137. As a direct and proximate result of Defendant's unlawful conduct, Plaintiff and Class members are entitled to recover actual, consequential, and punitive damages, as well as injunctive relief, and reasonable attorney's fees and costs, pursuant to 815 ILCS 505/10a and 815 ILCS 505/2z.

PRAYER FOR RELIEF

WHEREFORE Plaintiff, individually and on behalf of the Classes, requests that the Court:

A. Certify this case as a class action on behalf of the Classes defined above, appoint Plaintiff as the Class representative, and appoint the undersigned

counsel as Class counsel;

B. Award declaratory, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class members;

C. Award restitution and damages to Plaintiff and Class members in an amount to be determined at trial;

D. Award Plaintiff and Class members their reasonable litigation expenses and attorneys' fees to the extent allowed by law;

E. Award Plaintiff and Class members pre- and post-judgment interest, to the extent allowable; and

F. Award such other and further relief as equity and justice may require.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of any and all issues in this action so triable of right.

Plaintiff GRZEGORZ KAZMIERCZAK, individually and on behalf of all others similarly situated,

By: */s/ Thomas A. Zimmerman, Jr.*

Thomas A. Zimmerman, Jr.
Sharon A. Harris
Matthew C. De Re
Jeffrey D. Blake
Zimmerman Law Offices, P.C.
77 W. Washington Street, Suite 1220
Chicago, Illinois 60602
(312) 440-0020 telephone
www.attorneyzim.com
firm@attorneyzim.com

Arthur C. Czaja
Law Office of Arthur C. Czaja
7521 N. Milwaukee Ave.
Niles, Illinois 60714
(847) 647-2106 telephone
arthur@czajalawoffices.com

Counsel for Plaintiff and the Class and Subclass

COMMUNITY LOAN
SERVICING LLC

August 30, 2022

119 2 33833 **********AUTO**ALL FOR AADC 606
GRZEGORZ KAZMIERCZAK
[redacted]

Dear Grzegorz Kazmierczak,

Community Loan Servicing LLC ("CLS") understands the importance of protecting the information we maintain. We are writing to inform you of an incident that involved some of your information. This notice explains the incident, measures we have taken, and steps that you may consider taking.

CLS currently or previously serviced your mortgage loan. A security incident involving unauthorized access to our file servers was identified in early December 2021. Steps were immediately taken to contain the incident, notify law enforcement, and a forensic investigation firm was engaged. The investigation determined that an unauthorized person obtained access to files on our file storage servers from October 27, 2021 to December 7, 2021. The accessed files were then reviewed by our investigation team to identify the content. On August 24, 2022, the review process determined that some of your information, including your name and Social Security number, was included in the files. For some, the accessed files may also have included information provided in connection with a loan application, loan modification, or other items regarding loan servicing. The additional loan related information in the files is not the same for all individuals.

We wanted to notify you of this incident and assure you that we take it seriously. We engaged Kroll, a third party with monitoring expertise, to provide identity monitoring services at no cost to you for one year. The identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.
*You have until **November 29, 2022** to activate your identity monitoring services.*
Membership Number: **CIU873224-P**

For more information on your complimentary one-year membership, as well as additional steps you can take in response to the incident, please see the additional information provided in this letter.

We regret that this incident occurred and apologize for any inconvenience. Additional steps are being taken to further enhance our existing security measures. If you have questions about this notice, please call (855) 788-2606 from 8:00 a.m. – 5:30 p.m. Central Time, Monday through Friday (excluding major US holidays).

Sincerely,

Cristina Arroyo

Cristina Arroyo, SVP of Legal and Compliance
Community Loan Servicing LLC

EXHIBIT 1

ELN-15230-33833

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Triple Bureau Credit Monitoring
You will receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation
You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration
If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

If you prefer to activate these services offline and receive monitoring alerts via the US Postal Service, you may activate via our automated phone system by calling 1-888-653-0511, Monday through Friday, 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number located in your letter ready when calling. Please note that to activate monitoring services, you will be required to provide your name, date of birth, and Social Security number through our automated phone system.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity over the next 12 to 24 months. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.identitytheft.gov

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Additional information for residents of the following states:

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

Rhode Island: This incident involves 485 individuals in Rhode Island. Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: Rhode Island Attorney General's Office, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

West Virginia: You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.